USFQ LAW REVIEW
Volumen VIII, Núm. 1 • mayo 2021
ISSN: 2631-2573 • ISSN(e): 1390-8014



Los ejes centrales de la protección de datos: consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador

The central axes of data protection: consent and purpose. Criticisms and proposals towards a regulation of the protection of personal data in Ecuador

Felipe Nicolás Roldán Carrillo*

Recibido / Received: 28/01/2020
Aceptado / Accepted: 30/03/2021
DOI: https://doi.org/10.18272/ulr.v8i1.2184

Citación:
Roldán Carrilo, F.N. «Los ejes centrales de la protección de datos: consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador». *USFQ Law Review, Vol 8,* no 1, mayo de 2021, pp. 175 - 202, doi: 10.18272/ulr.v8i1.2184

* Abogado Investigador Independiente, casilla postal 17-1200-841, Quito 170901, Pichincha, Ecuador. Correo electrónico: felipe.roldan97@gmail.com ORCID iD: https://orcid.org/0000-0002-0673-7009

Resumen
El ordenamiento jurídico ecuatoriano busca integrar el nuevo fenómeno normativo que está viviendo el derecho de protección de datos personales. En la Asamblea Nacional actualmente se está discutiendo el Proyecto de Ley Orgánica de Protección de Datos. Su objetivo principal es proteger este derecho fundamental frente al inminente avance tecnológico para así brindar seguridad jurídica. En el siguiente artículo se hará un análisis de los principios de consentimiento del titular y finalidad del tratamiento de datos, con la intención de determinar qué estándar de protección se busca implementar. Esto se estudiará desde la óptica de la legislación comparada, examinando el modelo normativo europeo y estadounidense para finalizar con una crítica del posible impacto práctico que se podría generar en caso de entrar en vigencia dicha ley.

Palabras clave
Protección de datos, datos personales, estándar de protección, consentimiento, limitación de la finalidad, Proyecto de Ley Orgánica de Protección de Datos Personales

Abstract
The Ecuadorian legal system seeks to integrate the new regulatory phenomenon that the right to protection of personal data is experiencing. The National Assembly is currently discussing the Proyecto de Ley Orgánica de Protección de Datos. The main objective is to protect this fundamental right against the imminent technological advance in order to provide legal security. In the following article, an analysis will be made of the principles of consent and purpose limitation, with the intention of determining what protection standard is going to be implemented. This will be studied from the perspective of comparative legislation, examining the European and American regulatory model to end with a critique of the possible practical impact that could be generated if the law enters into force.

Keywords
Data protection, standard of protection, consent, purpose of treatment limitation, Proyecto de Ley Orgánica de Protección de Datos

1. Introducción

"*Personal data is the new oil of the internet and the new currency of the digital world*".[1]
Meglena Kuneva

Con el avance de las nuevas tecnologías y la globalización, cada día se torna más fácil vulnerar la privacidad de las personas y dar un mal uso de sus datos personales.[2] Estos cambios disruptivos presentan nuevos retos al derecho de protección de datos personales. Por eso, es de vital importancia regular el derecho a la protección de datos como un derecho autónomo, aunque muy pocos países han logrado darle dicho tratamiento.[3] Para dimensionar la falta de desarrollo, son 194 los países oficialmente reconocidos por la ONU, de los cuales tan solo 120 han incorporado legislación referente a la protección de datos.[4] Esta cifra equivale al 61% de países; no obstante, la gran mayoría no cuenta con un alto estándar de protección de datos o con leyes especializadas que lo regulen.[5]

El ordenamiento jurídico ecuatoriano es parte de este grupo de países que no cuentan con un estándar de protección de datos o con una ley especializada que lo regule, a pesar de recogerlo. La Constitución de la República y las leyes ecuatorianas son insuficientes al momento, de proteger este derecho fundamental. Actualmente, en la Asamblea Nacional se está discutiendo el Proyecto de Ley Orgánica de Protección de Datos Personales. El objetivo del presente trabajo es analizar cuál es el estándar de protección de datos que esta iniciativa busca implementar. El análisis del estándar se centrará específicamente en dos principios. Primero, está el principio de consentimiento, el cual constituye la piedra angular del derecho de protección de datos.[6] Segundo, está el principio de finalidad. Su importancia recae en la limitación en el actuar del responsable y encargado del tratamiento de datos a un fin específico.

Contar con un estándar de protección de datos personales presenta varias ventajas desde el punto de vista social, económico y político. Tutelar adecuadamente la privacidad de las personas es un reflejo de que una sociedad es democrática, reconoce y protege los derechos fundamentales.[7] Además, se

1 Meglena Kuneva, "Keynote Speech" en *Roundtable on Online Data Collection, Targeting and Profiling*, ed. Comisión Europea (Bruselas: Comisión Europea de Consumo, 2009), 2.

2 Concepción Conde Ortiz, *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad*, (Madrid: Dykinson, 2016), 19-20.

3 Ramón Oró Badia, *La protección de datos*, (Barcelona: Editorial UOC, 2015), 11.

4 David Banisar, "Article 19: Global Campaign for Free Expression", *National Right to Information Laws, Regulations and Initiatives 2018* (diciembre 2018): 1, http://dx.doi.org/10.2139/ssrn.1951416..

5 Payal Arora, "General Data Protection Regulation—a Global Standard? Privacy Futures, Digital Activism, and Surveillance Cultures in the Global South", *Surveillance and Society* 17 no. 5 (diciembre 2019): 718, https://doi.org/10.24908/ss.v17i5.13307..

6 Ana Garriga Domínguez, *Nuevos Retos para la Protección de Datos. En la Era del Big Data y de la computación ubicua* (Madrid: Dykinson, 2016), 153.

7 José Luis Piñar Mañas, "¿Existe privacidad?", en *Protección de Datos Personales, Compendio de Lecturas y Legislación*, ed. H. Cámara de Diputados (México: Tiro Corto Editores, 2010), 19-20.

hace un llamado al inversor extranjero y a otros países, a invertir en Ecuador. Si se busca la libre circulación de personas, mercancías y capitales, debería ser igual con los datos personales. Debería existir un flujo libre, donde exista una normativa que regule efectivamente el tratamiento de datos, y una autoridad competente que cuente con las herramientas necesarias para poder sancionar cualquier vulneración a los datos personales del titular.

Esto ha sido mermado por la falta de normativa especializada en esta materia. En el año 2016 se suscribió el Protocolo de Adhesión de Ecuador al Acuerdo Comercial Multipartes con la Unión Europea, donde se acordó desarrollar un nivel de protección adecuado para el flujo trasfronterizo de datos personales. Al no tener una ley que regule el tratamiento de datos personales ni una autoridad competente, se presentan dificultades a empresas que deben lidiar con la transferencia internacional de datos personales, pues no hay seguridad jurídica.[8] Además, no existe una verdadera protección para los ciudadanos. Cada día se vulnera este derecho fundamental de los ecuatorianos de distintas maneras, ya sea por la venta ilegal de datos, acoso de operadoras telefónicas, entre otras.

Para los efectos mencionados anteriormente, se llevará a cabo una metodología descriptiva y analítica. En el trabajo se empezará señalando la importancia de la regulación del derecho de protección de datos personales y por qué nuestro ordenamiento jurídico tiene falencias. También se explicará por qué es elemental desarrollar un estándar adecuado de protección respecto del consentimiento del titular y poner un límite a la finalidad de su tratamiento [§ 2]. Después se hará un estudio del estándar de protección de datos en la Unión Europea y Estados Unidos, para ver cómo es el estándar de consentimiento y finalidad en estos sistemas legales [§ 3]. Por último, un análisis al estándar de protección de datos personales sobre el consentimiento y finalidad y cuáles son las críticas y propuestas en el Ecuador con respecto al Proyecto de Ley Orgánica de Protección de Datos Personales [§ 4].

2. Protección de datos: Importancia de su regulación

2.1 Antecedentes y falencias del sistema legal ecuatoriano

A nivel mundial se está generando consciencia de crear un marco normativo para dar especial protección y correcto tratamiento a los datos personales. En mayo de 2016, el Consejo de Europa promulgó el Reglamento General de Protección de Datos (en adelante RGPD) que entró en vigencia el 25 de

8 Derechos Digitales y APC, "Requisitos mínimos para la Ley de Protección de Datos Personales de Ecuador Asociación para el Progreso de las Comunicaciones", *Access Now*, 29 de mayo de 2020. https://www.apc.org/es/pubs/requisitos-minimos-para-la-ley-de-proteccion-de-datos-personales-de-ecuador.

mayo de 2018.[9] El objetivo principal es el fortalecimiento de la normativa de protección de datos y actualización de las antiguas directrices europeas que no hacían un frente directo a los nuevos desafíos tecnológicos.[10] El RGPD ha creado un nuevo estándar, por lo que se le considera como un punto de referencia para que en otras legislaciones se empiecen a desarrollar normas específicas de protección de datos. En Latinoamérica, Brasil decidió elevar el estándar de protección de datos para cumplir con los parámetros del RGPD, y Chile está debatiendo un proyecto de ley para adecuarse al RGPD.[11]

Existen incentivos económicos para que los Estados incorporen en su legislación un marco adecuado de protección de datos.[12] Por ejemplo, contar con un sistema óptimo de protección, abre el mercado para inversiones internacionales y actividades empresariales que implican la transferencia de datos personales, lo que podría generar un espacio más competitivo para las TIC.[13] Un cuerpo normativo integral y moderno de protección de datos, promueve "la confianza y la certeza jurídica en el uso de datos como base de la economía y la innovación en la sociedad de la información",[14] permitiendo así la integración tecnológica y desarrollo económico. Igualmente, hay una reducción de costos en abogados y litigios, ya que al establecer un estándar internacional no se debe incurrir en asesoría legal para consultar la regulación de cada país y se evita posibles sanciones.

Ecuador es una excepción a este nuevo fenómeno normativo que se vive a nivel internacional, aunque se debe recalcar que el ordenamiento jurídico reconoce y protege al derecho a la protección de datos. Este derecho se lo reconoce como un derecho constitucional, en el artículo 66 numeral 19 de la Constitución,[15] como uno de los derechos de libertad. Según lo prescito en la norma mencionada, este derecho incluye el acceso, la decisión sobre la información y protección de datos de carácter personal. Para el tratamiento necesariamente se requiere del consentimiento del titular o de un mandato legal,[16] siendo este la regla general para legitimar cualquier tratamiento que otorgue a los datos obtenidos.

9 Reglamento General de Protección de Datos 2016/679 [RGPD], Unión Europea: Parlamento y Consejo Europeo, 27 de abril de 2016.

10 Ana Isabel Herrán Ortiz, "Aproximación al derecho a la protección de datos personales en Europa. El Reglamento General de Protección de Datos personales a debate", *REDS 8*, (enero 2016): 180–182, https://dialnet.unirioja.es/servlet/articulo?codigo=6140105.

11 Paulina Bojalil y Carlos Vela Treviño, "Despuntan las reformas en materia de protección de datos en América Latina", *Abierto al Público*, 12 de febrero de 2019. https://blogs.iadb.org/conocimiento-abierto/es/proteccion-de-datos-gdpr-america-latina/.

12 Ibid.

13 Antonio Troncoso Reigada, "El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibro en los modelos de protección de datos a nivel Internacional", *Revista Internacional de Protección de Datos Personales 1* (Julio 2012): 30-31*, https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/10_Antonio-troncoso_FINAL.pdf*.

14 Derechos Digitales y APC, "Requisitos mínimos".

15 Artículo 66 numeral 19, Constitución de la República del Ecuador, R.O. 449, 20 de octubre de 2008.

16 Id., Artículo 92.

A primera vista, el reconocimiento como un derecho constitucional genera seguridad, pero el desarrollo legal de estas protecciones es insuficiente. Existen distintas razones por las cuales se puede asegurar esto. Primero, no hay una definición del concepto de datos personales en la Constitución y demás normas jurídicas. Segundo, los mecanismos que se han implementado para proteger este derecho resultan ineficientes.

Para Lorena Naranjo, directora de la Dirección Nacional de Registro de Datos Públicos (en adelante DINARDAP), por el momento, el *habeas data* es el mecanismo adecuado para proteger el derecho a la protección de datos personales.[17] La Corte Constitucional manifiesta que:

> [Es] un mecanismo de satisfacción urgente para que las personas puedan obtener el conocimiento de los datos a ellos referidos, y advertirse sobre su finalidad, sea que dicha información conste en el registro o banco de datos público o privado.[18]

La finalidad de esta garantía es la protección del derecho a la intimidad del titular, ya que no toda la información relativa a este tiene el carácter de pública y por tanto no puede ser divulgada libremente.[19] Otra sentencia importante de la Corte Constitucional es el precedente jurisprudencial obligatorio 001-14-PJO-C. Se reconoce al *habeas data* como un mecanismo de garantía del derecho a la protección de datos personales y aparte desarrolla el concepto de autodeterminación informativa que es la verdadera expresión de este derecho.[20]

A pesar de la intención del legislador y la interpretación que ha dado la Corte Constitucional, en la práctica se presentan dificultades. Partiendo del hecho de que la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (en adelante LOGJCC) no establece un momento oportuno para plantear esta acción. Para poder plantearla se hace alusión a la espera de un plazo razonable, lo que no resuelve esta problemática relativa al tiempo.

El artículo 51 de la LOGJCC, al referirse a la legitimación activa, faculta a personas jurídicas para presentar esta acción.[21] De esta manera, se desnaturaliza el objetivo de la acción, pues son ellas quienes pueden vulnerar los derechos de personas naturales por el mal manejo de datos. Por último, dada la naturaleza de la acción, esta es una medida *ex post*, a la cual acude el ciuda-

17 Ver, Naranjo, Lorena. "Habeas Data es la acción jurídica para proteger los datos personales hasta tener una legislación", Dirección Nacional de Registro de Datos Públicos, 7 de octubre de 2020. https://www.dinardap.gob.ec/habeas-data-es-la-accion-juridica-para-proteger-los-datos-personales-hasta-tener-una-legislacion/.

18 Sentencia 025-15-SEP-CC, Corte Constitucional del Ecuador, 4 de febrero de 2015, pág. 11.

19 Sentencia 182-15-SEP-CC, Corte Constitucional del Ecuador, 3 de junio de 2015, pág. 15.

20 Sentencia 001-14-PJO-C, Corte Constitucional del Ecuador, 23 de abril de 2015, párr. 27-30.

21 Artículo 51, Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, [LOGJCC], R.O. Suplemento 52, 22 de octubre de 2009.

dano únicamente "cuando se da un uso de información personal que viole un derecho constitucional".[22]

Por otra parte, en otros cuerpos normativos se trata el derecho a la protección de datos como la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, la Ley del Sistema Nacional del Registro de Datos Públicos y el Código Orgánico Integral Penal. Estas normas hacen una breve referencia a la protección de datos personales; sin embargo, no especifican cómo tratarlo y protegerlo. Además, no hay una autoridad competente en materia de protección de datos. Si se establecen normas jurídicas que traten la protección de datos personales, es necesario crear un órgano público independiente cuya función sea la supervisión del cumplimiento efectivo de los derechos del titular.[23]

El propósito de una ley específica de protección de datos es desarrollar con mayor profundidad esta materia. Se deben definir: conceptos generales, principios, derechos, deberes, mecanismo de protección y sanciones. Por eso, la Constitución, los distintos cuerpos normativos que contemplan este derecho y el *habeas data*, resultan insuficientes en el auxilio del derecho a la protección de datos personales.

2.2. Importancia del consentimiento y finalidad en la protección de datos personales

En la actualidad una persona puede firmar en un año muchos más contratos que sus abuelos a lo largo de su vida.[24] El problema principal en la mayoría de los casos se debe a que el titular no conoce ni autoriza la recolección y tratamiento de sus datos personales. En el supuesto de consentirlo, no siempre conoce la finalidad del tratamiento de sus datos o si se los utiliza para fines distintos a los de su recolección. Dada la facilidad de acceso a internet y el desarrollo de nuevas tecnologías, vulnerar el derecho a la protección de datos personales de las personas resulta fácil. Hay un sinnúmero de casos donde se da un uso no autorizado de datos personales o inadecuado manejo de estos.

Para entender la gravedad de esto se expondrán tres casos icónicos, actuales y controvertidos. Son un reflejo del problema principal: el titular no ha consentido el tratamiento de sus datos personales; o, la aceptación al manejo de datos se ha extrapolado a finalidades distintas y ulteriores a la consensuada.

22 Id., Artículo 50.

23 Luis Enríquez Álvarez, "Paradigmas de la protección de Datos Personales en Ecuador. Análisis del Proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales", *Foro 27* (Febrero 2018): 46, https://revistas.uasb.edu.ec/index.php/foro/article/view/500.

24 Iñigo de la Maza Gazmuri y Rodrigo Momberg Uribe, "Términos y condiciones: Acerca del supuesto carácter contractual de las autorizaciones para el tratamiento de datos personales en sitios web", *Revista Chilena De Derecho y Tecnología* 6 (diciembre 2017): 26, http://dx.doi.org/10.5354/0719-2584.2017.46226.

El primer caso se relaciona con la compañía Facebook. La Comisión Federal del Comercio de Estados Unidos multó a Facebook con $5.000 millones de dólares por irregularidades en su sistema de privacidad.[25] Este escándalo se dio a conocer por la actividad de *Cambridge Analytica* que fue una empresa dedicada al análisis de datos políticos. En el año 2014 esta empresa tuvo acceso a los perfiles de Facebook a través de una aplicación llamada *This Is Your Digital Life*, donde los usuarios al descargarla autorizaban a la empresa a acceder a su información personal.[26] Con esta, tenía como objetivo influenciar a los usuarios en sus decisiones políticas proporcionando determinada información de acuerdo con el perfil levantado.

De este modo y por las políticas de Facebook, la aplicación podía acceder a los datos personales de usuarios que consintieron su tratamiento de forma directa y a los de su círculo de amigos de forma indirecta. Alrededor de 270.000 usuarios consintieron compartir sus datos y, por ende, se manejó indebidamente la información de más de 85 millones de usuarios.[27] En este caso, se extrapoló el consentimiento del titular y la finalidad para la cual fueron recabados los datos personales.

El segundo caso trata sobre la multinacional Google que fue multada por la Comisión Nacional de la Informática y las Libertades, de Francia, con una sanción de $50 millones de euros. La investigación nace de reclamos colectivos por parte de *La Quadreature du Net* y *None of Your Business*. Ambas asociaciones mencionaron que el buscador de Google no contaba con una base legal apta para procesar datos personales de los usuarios del servicio, sobre todo en temas publicitarios.[28] Este reclamo procedió por la falta de información proporcionada y falta de consentimiento del titular para que se personalice publicidad de acuerdo con su perfil. En este caso, la aceptación del titular no es específica, ya que se encamina al usuario a dar su consenso en bloque para todos los fines que quiera dar la empresa y no se limita una finalidad clara.

Por último, la compañía de telecomunicaciones TIM fue multada por la Agencia de Protección de Datos italiana por un valor de $27.8 millones de euros. Luego del caso de Google, esta sería la segunda sanción más alta en Europa en aplicación del RGPD.[29] Esta investigación inicia ya que distintos usuarios y

25 "La multa récord de US$5.000 millones que deberá pagar Facebook en EE. UU", *BBC News Mundo*, 24 de julio de 2019. https://www.bbc.com/mundo/noticias-49093124.

26 Carole Cadwalladr y Emma Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", *The Guardian*, 17 de marzo de 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

27 Amnistía Internacional, "Gigantes de la vigilancia: La amenaza que el modelo de negocios de Google y Facebook representa para los Derechos Humanos", *Amnistía Internacional*, 5 de diciembre de 2019, 15 de septiembre de 2020. https://www.amnesty.org/download/Documents/POL3014042019SPANISH.PDF.

28 Europa Press, "Francia multa con 50 millones a Google por infringir las normas de protección de datos", *La Vanguardia*, 21 de enero de 2019. https://www.lavanguardia.com/tecnologia/20190121/454234917044/francia-multa-google-50-millones-infringir-proteccion-datos.html.

29 Gonzalo Sánchez.Jara, "Italia impone la segunda multa más alta en Europa por infracción del RGPD: 27,8 millones de euros", *Noticias RGPD*, 19 de febrero de 2020. https://rgpdblog.com/italia-impone-la-segunda-multa-mas-alta-en-europa-

prospectos de la operadora presentaron quejas ante la autoridad entre el 2018 y 2019 por un manejo agresivo e ilegítimo de la estrategia de marketing de la empresa.[30] A lo largo de la investigación se descubrieron varias infracciones, no se mencionarán todas.

Durante el período 2018-2019, TIM y sus agentes comerciales realizaron campañas de telemarketing a 13 millones de clientes y potenciales clientes, sin su consentimiento.[31] Incluso, un solo individuo en un mes llegó a recibir más de 150 llamadas por parte de las operadoras. También existía una indebida gestión de las listas de exclusión de personas que se opusieron a dichas llamadas. A su vez, manejaban formularios de recopilación de datos personales donde se solicitaba un único consentimiento, pero para diversas finalidades.[32]

De estos tres casos se pueden sacar dos conclusiones principales. La primera y la lógica, tanto titulares de datos personales como empresas no han interiorizado la importancia de ambos principios, lo que se traduce en desconocimiento e incumplimiento de la norma. La segunda y menos viable, los estándares de protección de datos respecto del consentimiento y finalidad, no son lo suficientemente claros. Por eso, la intención en esta sección es demostrar la importancia de estos principios y describir cuál es el estándar de protección que se busca otorgar a los mismos.

La doctrina[33] y jurisprudencia[34] reconocen el derecho a la protección de datos como un derecho fundamentado en la autodeterminación informativa. Es la facultad de una persona para elegir y tomar decisiones respecto de sus datos personales. El titular de datos debe buscar aquella línea de equilibrio entre mantener un ámbito íntimo y uno privado de aquellos datos que deben ser conocidos públicamente.[35] Con base en esto, Troncoso asegura que el consentimiento del titular es un pilar esencial del contenido de este derecho.[36]

Existen casos en los que el tratamiento de datos va mas allá del propósito de su recolección y el titular no lo ha consentido. Debe existir una relación directa entre los datos personales recogidos y la finalidad de su obtención, por

por-infraccion-del-rgpd-278-millones-de-euros/.

30 Medida correctiva y sancionadora contra TIM S.p.A 9256486, Garante de la Protección de Datos Italiano, 15 de enero de 2020, pág. 28.

31 Id., pág. 1.

32 Id., pág. 2-13.

33 Jed Rubenfeld, "The right of Privacy". *Harvard Law Review*. Vol. 4 (Febrero 1989): 750-751,

https://doi.org/10.2307/1341305..

34 Sentencia 1 BvR 209, 269, 362, 420, 440, 484/83, Tribunal Federal Alemán, Primera Sala, 15 de diciembre de 1983, párr. 106, 144-146.

35 Liliana Minardi Paesani, *Direito e Internet: liberdade de informação, privacidade e responsabilidade civil* (São Paulo: Atlas, 2014), 28.

36 Antonio Troncoso Reigada, *La Protección de Datos Personales. En búsqueda del* equilibrio, (Madrid: Tirant Lo Blanch, 2011), 461.

lo que la finalidad es un segundo pilar del contenido esencial de este derecho, mediante el cual se limita el manejo de datos.[37]

Esta materia se encuentra delimitada por distintos principios rectores, entre ellos el consentimiento y la finalidad que deben ser observados por todo aquel que dé tratamiento a datos personales.[38] El consentimiento es la facultad del titular para decidir acerca de sus datos.[39] Mientras que la finalidad del tratamiento de datos exige un propósito determinado, explícito y legítimo.[40] Así, la clara determinación y correcta regulación de ambos principios es esencial para tener un modelo normativo que haga efectivo el ejercicio de este derecho.[41]

Tomando como referencia todo lo expuesto anteriormente, es necesario definir los estándares de protección y explicar por qué están construidos de dicha manera, ya que a través del cumplimiento de estos se garantiza un ejercicio pleno del derecho de autodeterminación. Un estándar es una serie de requisitos que funcionan como una herramienta para dar tratamiento a los datos personales.[42] En el derecho de protección de datos, estos son requisitos mínimos, pero indispensables. Omitir uno de estos evidentemente vulneraría el derecho fundamental a la protección de datos personales. El Tribunal Constitucional de España afirma que "ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin". [43]

El consentimiento es la manifestación de la voluntad, constituye ciertamente la forma ideal de exteriorizarla. En el derecho a la protección de datos personales se traduce en la aceptación o rechazo del titular al tratamiento de sus datos personales.[44] Distintos autores como Garriga[45], Rebollo y Serrano[46], Troncoso[47], aseguran que el consentimiento debe cumplir con ciertas características. Estas responden al estándar de consentimiento que debe ser libre, específico, inequívoco e informado.

37 Garriga, *Nuevos Retos*, 97.

38 Troncoso, *En búsqueda del equilibrio*, 394.

39 Paloma de Barrón Arniches, "La pérdida de privacidad en la contratación electrónica (entre el Reglamento de protección de datos y la nueva Directiva de suministro de contenidos digitales)", *Cuadernos Europeos de Deusto* (octubre 2019): 55-57, https://doi.org/10.18543/ced-61-2019pp29-65.

40 Lucrecio Rebollo Delgado y María Mercedes Serrano Pérez, *Introducción a la Protección de Datos* (Madrid: Dykinson, 2008), 144.

41 Francisco Javier Puyol Montero, "Los Principios del Derecho a la Protección de Datos", en *Reglamento general de protección de datos*, ed. José Luis Piñar Mañas (Madrid: Editorial Reus, 2017), 135-136.

42 Adrián Palma Ortigosa, "Contexto normativo de la protección de datos personales", en: *Protección de datos, responsabilidad activa y técnicas de garantía*, ed. Juan Pablo Murga Fernández et al. (Madrid: Editorial Reus, 2018), 22.

43 Sentencia 292/2000, Tribunal Constitucional Español, 30 de noviembre de 2000, pág. 21.

44 Catalina Frigeiro Dattwyler, "Mecanismos de regulación de datos personales: una mirada desde el análisis económico del derecho", *Revista Chilena De Derecho y Tecnología* 7 (diciembre 2018): 64, http://dx.doi.org/10.5354/0719-2584.2018.50578.

45 Garriga, *Nuevos Retos*, 185.

46 Rebollo y Serrano, *Introducción a la protección de datos*, 126-128.

47 Troncoso, *En búsqueda del* equilibrio, 391.

Primer requisito: consentimiento libre. El titular de datos debe proporcionar su consentimiento de manera voluntaria, no puede obtenerse coactivamente.[48] Segundo elemento: consentimiento específico. La aceptación del tratamiento de datos por parte del titular debe estar encaminada a una finalidad concreta. Tercer requisito: consentimiento informado. El titular debe ser "consciente y entender los hechos y las implicaciones que se derivan de su prestación, lo que relaciona directamente con la noción de control y autodeterminación".[49] Cuarto requisito: consentimiento inequívoco. No cabe duda alguna sobre la voluntad del titular de aceptar el tratamiento de datos personales.

Aparte del consentimiento del titular, la legitimidad del tratamiento de datos personales también puede ser otorgada por mandato legal, ejecución de un contrato y orden de autoridad competente. Pese a existir distintas formas de legitimar el tratamiento de datos personales, el consentimiento es la regla general y un pilar fundamental, el cual será analizado a lo largo del presente trabajo.

Partiendo del hecho de que existen distintas maneras para que el tratamiento sea legítimo, estas deben estar encaminadas a un propósito. Es aquí donde radica la importancia del principio de finalidad. Este se exterioriza como una garantía fundamental mediante la cual se presenta a los titulares de los datos personales la posibilidad de controlar el manejo de estos. Para Garriga, este principio ofrece una respuesta "precisa y concreta a la cuestión de para qué van a ser utilizados, impidiendo además usos diferentes o incompatibles con el consentido".[50] De conformidad con Troncoso[51], el estándar de protección otorgado a este principio es que sea una finalidad: legítima, determinada y explícita. La razón de este es introducir un criterio de proporcionalidad y racionalidad antes de dar tratamiento a los datos personales que se van a recabar.[52]

Una finalidad legítima es la causa de justificación del tratamiento de datos personales, la cual se debe ajustar a los preceptos establecidos en cada ordenamiento jurídico. Incluso si el manejo de datos es el correspondiente a la finalidad, si este no es concordante con lo prescrito en el ordenamiento jurídico, no es legítimo. También es necesario que la finalidad sea determinada, es decir que no se podría establecer finalidades generales, vagas o inconcretas. Último elemento, finalidad explícita. Se debe proporcionar toda la información al titular de datos, ya que con esta podrá tener control de la información y prestar su consentimiento. Este estándar debe ser analizado a la par con el principio

48 Garriga, *Nuevos Retos*, 187.

49 Carlos Trujillo Cabrera, "Las bases de legitimación del tratamiento de datos personales. En especial, el consentimiento" en: *Protección de datos, responsabilidad activa y técnicas de garantía*, ed. Juan Pablo Murga Fernández (Madrid: Editorial Reus, 2018), 57.

50 Garriga, *Nuevos Retos,* 97.

51 Troncoso, *En búsqueda del* equilibrio, 395-398.

52 Santiago Milans del Bosch y Hugo Jordán de Urríes, "La incidencia de la protección de datos personales en la actuación de la Administración local", *Fundación Democracia y Gobierno Local* (octubre 2004): 107-109, http://hdl.handle.net/10873/160..

de minimización de datos, que establece que estos deben ser adecuados, pertinentes y limitados a la finalidad.

3. Derecho comparado: análisis del consentimiento y finalidad

La protección de datos personales atraviesa una metamorfosis normativa a nivel mundial. Son dos modelos de protección por los que se puede optar al momento de incorporar estos cambios legislativos: europeo y estadounidense. Son experiencias internacionales importantes y la manera en que protegen este derecho fundamental es distinta. En el modelo europeo la protección de datos personales se encuentra debidamente regulada. Existe una autoridad de inspección y de sanción. En cambio, en el modelo estadounidense, la autorregulación o regulación mínima es el principal componente. No hay una autoridad estatal que se encargue de velar por este derecho fundamental. Los titulares deberán acudir a la instancia judicial para solicitar determinar la responsabilidad de la empresa por su actuar y solicitar una indemnización.

El cuerpo normativo por analizar en el marco europeo es el RGPD. Mientras que en Estados Unidos se tomará como referencia el *California Consumer Privacy Act* (en adelante CCPA). Es importante analizar ambos cuerpos normativos porque son los más actualizados en materia de protección de datos personales. En esta sección se analizará cuáles son los estándares de protección del consentimiento y finalidad en ambos sistemas.

3.1. Unión Europea: Reglamento General de Protección de Datos

Whitman explica que en el modelo europeo la protección de datos es la manera en la que se garantiza el derecho a ser respetado y protege la dignidad de la persona.[53] El objetivo del RGPD, es garantizar un nivel adecuado y coherente de protección de datos de personas físicas en toda la Unión Europea.[54] En el RGPD, el consentimiento juega un rol importante, pues cambia el sistema de registro y tratamiento de datos en todos los servicios.[55] El consentimiento es el leal ejercicio de la autodeterminación informativa, esta es la razón de ser de este modelo normativo.[56] Por otro lado, se introduce un nuevo estándar de finali-

53 James Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty", *Yale Law Review* 113 (diciembre 2003): 11-15, http://dx.doi.org/10.2139/ssrn.476041.

54 Herrán, "Aproximación", 180-182.

55 Natalia Martos, "Principios (Arts.6-11)", en *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos: adaptado al Proyecto de Ley Orgánica de Protección de Datos de 10 de noviembre de 2017*, ed. José López Calvo (Madrid: Wolters Kluwer, 2018), 349.

56 Sentencia 1 BvR 209, 269, 362, 420, 440, 484/83, párr. 144-146.

dad, asegurando que los datos recabados sean determinados, explícitos, legítimos.[57] A continuación, se desarrollarán los estándares de protección de datos.

3.1.1. Consentimiento

El RGPD establece seis mecanismos para legitimar el tratamiento de datos personales. Según lo prescrito en el artículo 6 son: 1) consentimiento del titular; 2) el titular es parte de una relación contractual en la que se necesita procesar sus datos personales; 3) una obligación legal que exige al responsable el tratamiento de datos; 4) una necesidad de protección de los intereses vitales del titular u otras personas; 5) interés público o ejercicio de poderes públicos; y 6) satisfacer intereses legítimos perseguidos por el responsable del tratamiento o terceros. Según Trujillo, de estos seis presupuestos, el consentimiento es la regla general al momento de tratar datos personales.[58]

Para que un consentimiento sea válido, en primer lugar, el titular de datos debe tener la capacidad jurídica establecida en materia civil, caso contrario desde un inicio el consentimiento tendrá un vicio de invalidez.[59] Es necesario establecer el estándar de protección de datos que el RGPD busca dar a este principio en el artículo 4 numeral 11. La manifestación de voluntad del titular debe tener cuatro criterios indispensables: libre, específica, informada e inequívoca.[60]

Primer elemento: consentimiento libre. Es la decisión encaminada del titular a buscar un objetivo específico y permitir el tratamiento de sus datos personales. El Grupo de Trabajo del Artículo 29 menciona que "el interesado puede elegir una opción real y no hay ningún riesgo de engaño, intimidación, coerción o consecuencias negativas significativas en caso de que no consienta".[61] De lo mencionado, hay dos situaciones en las que la libertad del consentimiento puede verse comprometida.

Primero, cuando se trata de vicios del consentimiento. Estos responden a error, fuerza o dolo.[62] Segundo, ciertos casos en los que el consentimiento libre puede verse en juicio de duda, sobre todo en situaciones donde el titular se encuentra en subordinación. Este desequilibrio en la relación, responsable del tratamiento y titular, puede ser de carácter económico o de cualquier

57 Joaquín Muñoz Ontier, "Disposiciones Generales (Arts.1-5)", en *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos: adaptado al Proyecto de Ley Orgánica de Protección de Datos de 10 de noviembre de 2017*, ed. José López Calvo (Madrid: Wolters Kluwer, 2018), 360-363.

58 Trujillo, "Las bases de legitimación", 52.

59 Agencia de los Derechos Fundamentales de la Unión Europea, *Manual de legislación europea en materia de protección de datos* (Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2019), 130.

60 Artículo 4 numeral 11, RGPD.

61 Resolución 15/2011, Grupo de Trabajo del Artículo 29 [sobre la definición de consentimiento para percatarse de lo manifestado], 13 de julio de 2011.

62 Agencia de los Derechos Fundamentales, *Manual de legislación europea*, 130.

otra índole, por ejemplo, en temas laborales. En estos casos únicamente hay un verdadero consentimiento libre cuando se trata de circunstancias excepcionales, donde la acepción o rechazo no tengan consecuencias contra ellos.[63]

Según el considerando 43, tampoco podrá ser libre si el titular no tiene la opción de revocar su consentimiento o en caso de hacerlo, sufra una consecuencia negativa.[64] *Ergo* si este requisito se encuentra sujeto a condiciones, existe coerción de por medio, no se goza de una libre elección o la cancelación del consentimiento acarrea perjuicio alguno, se entenderá que el consentimiento no es libre.[65]

Segundo: consentimiento específico. Se cumple cuando se solicita una autorización para una o varias finalidades concretas y específicas.[66] Según lo prescrito en el artículo 7 numeral 2, para que se hable de un consentimiento específico este tendrá que ser inteligible.[67] Es decir, el titular debe determinar qué datos personales serán objeto de tratamiento, cómo se llevará a cabo este manejo y para qué fines estarán destinados. Esta característica se correlaciona directamente con el principio de finalidad. No se podrá consentir para finalidades generales, indeterminadas o ilegítimas.[68]

Tercer elemento: consentimiento informado. Se cumple cuando el titular cuenta con información suficiente sobre el tratamiento de datos, previo a tomar su decisión.[69] Esta condición asegura el control de la situación, que el titular esté consciente y comprenda las implicaciones que conlleva aceptar el tratamiento. La información otorgada al titular debe cumplir con los requisitos de los principios de transparencia y calidad de datos.

Los artículos 13 y 14 establecen la información que debe ser facilitada al titular.[70] Debe ser fácil de comprender y precisa, redactada en un lenguaje claro y sencillo, sin tecnicismos.[71] El titular debe conocer como mínimo cuál es la finalidad del tratamiento de sus datos personales y quién es el responsable de este. Incluso, se deben informar las consecuencias que pueden derivar por no consentir el tratamiento de datos personales. Si la información no cuenta con estas características y no brinda al titular el control de la situación, no se cumplirá este requisito.

---

63 Dictamen 2/2017, Grupo de Trabajo del Artículo 29 [sobre el tratamiento de datos personales en el trabajo], 8 de junio de 2017.
64 Considerando 42, RGPD.
65 Id., Considerando 42.
66 Id., Artículo 6 numeral 1.
67 Id., Artículo 7 numeral 2.
68 Id., Artículo 5 numeral 1 literal b.
69 Id., Artículo 7 numeral 3.
70 Id., Artículo 13 y 14.
71 Resolución 15/2011, pág. 19.

Cuarto requisito: consentimiento inequívoco. Se cumple cuando no se desprende duda sobre la intensión del titular al momento de consentir el tratamiento de sus datos personales y que el consentimiento ha sido emitido por el verdadero titular de datos. Se busca certeza total. El artículo 7 numeral 1 prescribe que la prueba del consentimiento es un elemento clave y necesario para demostrar la validez de este.[72] Solo así el responsable puede declarar que el titular brindó su consentimiento.

El nuevo elemento que el RGPD introduce a este requisito, es la prestación del consentimiento a través de una acción clara afirmativa o una declaración. Debe haber una conducta activa por parte del titular. De esta manera, se eliminaría cualquier interpretación arbitraria. Como se puede observar, este estándar busca reforzar el objetivo general del RGPD, la protección jurídica de las personas y el desarrollo de la autodeterminación informativa.

3.1.2. Finalidad

El artículo 4 numeral 3 señala que debe existir una limitación al tratamiento de datos.[73] Esta es una garantía jurídica mediante la que se asegura al titular un adecuado manejo de sus datos personales. La manera en la que se limita el tratamiento de datos en el RGPD es a través del principio de finalidad. Por eso, en el artículo 5 numeral 1 literal b se ha establecido un estándar para que se considere un procesamiento de datos legítimo. Este prescribe lo siguiente: "los datos personales serán recogidos con fines determinados, explícitos y legítimos".[74] Se desprenden tres elementos importantes a tomar en consideración: fin determinado, explícito y legítimo.

Para que la finalidad sea válida debe ser legítima. Esto se cumple cuando el tratamiento está amparado por ordenamiento jurídico. Una finalidad que no se apegue a lo contemplado en la norma será ilegítima. El segundo requisito establece un fin determinado. Lo que busca este mecanismo es que el responsable del tratamiento de datos determine un propósito que debe ser específico y concreto. No se aceptarán finalidades genéricas y amplias. Según el considerando 39 del RGPD, dicha finalidad procede al momento de recopilar los datos personales del titular.[75] Esto se concatena con el deber de información y con el consentimiento informado, en el sentido en que se facilita la información específica por la que se están recolectando sus datos.

Último requisito: finalidad explícita. Se cumple cuando el responsable del tratamiento de datos a través del fichero presenta información en lenguaje

72 Id., Artículo 7 numeral 1.
73 Id.
74 Id., Artículo 5 numeral 1 literal b.
75 Id., Considerando 39.

claro, sencillo y libre de tecnicismos. Existe una relación con el consentimiento inequívoco del titular, pues no le quedaría duda alguna sobre el motivo principal del tratamiento de datos.

Este principio debe analizarse junto con el principio de minimización de datos. De acuerdo con lo prescrito en el artículo 5 numeral 1 literal c, los datos personales deben ser "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados".[76] Instaurando mayor rigurosidad en el tratamiento de datos, no solo se necesitará que se cumplan los tres elementos del estándar, sino que estos sean pertinentes, limitados y adecuados.

Otro elemento contenido en el artículo 5 numeral 1 literal b para que la finalidad sea válida, es que los datos recogidos no podrán ser "tratados ulteriormente de manera incompatible con dichos fines".[77] En ciertas ocasiones, a los datos personales se les puede dar otra finalidad adicional a la inicial, siempre que sea compatible con la inicial.[78] Significa que se admite el uso de datos personales para ciertos casos que surgen con posterioridad, cuando tenga una finalidad compatible.[79]

Cuando se pretenda dar un fin adicional y diferente, y este no se rige al estándar de compatibilidad, se debe otorgar un nuevo consentimiento que debe cumplir todos los requisitos mencionados anteriormente. No se puede extender la aceptación del titular para finalidades ulteriores, bajo la premisa de que en un inició consintió el tratamiento para una finalidad legítima al operador. Cada nueva finalidad, necesariamente, deberá tener una aceptación propia.

Ahora, ¿cómo se analiza el estándar de compatibilidad? El responsable del tratamiento de datos, para dar un tratamiento adecuado y legítimo tiene que realizar un análisis fáctico-jurídico. Según el considerando 50[80] y lo prescrito en el artículo 6 numeral 4 del RGPD,[81] son cinco factores a tomar en consideración: 1) la existencia de una relación entre el fin inicial con el fin ulterior; 2) análisis del contexto por el cual fueron recogidos los datos personales con relación al titular y su relación al responsable sobre el nuevo consentimiento; 3) determinar la naturaleza de los datos personales; 4) establecer las consecuencias jurídicas que acarraría al titular el tratamiento posterior; y 5) identificar la existencia de las debidas garantías en el tratamiento de ambas finalidades.

El RGPD establece una serie de requisitos que deben ser observados con cautela para que no se vulnere de ninguna manera el derecho fundamental a la protección de datos. El mecanismo principal es el estándar que debe mante-

76 Id., Artículo 5 numeral 1 literal c.
77 Id., Artículo 5 numeral 1 literal b.
78 Id., Artículo 5.
79 Agencia de los Derechos Fundamentales, *Manual de legislación europea*, 140.
80 Considerando 50, RGPD.
81 Id., Artículo 6 numeral 4.

ner el responsable del tratamiento, mismo que debe ir en consonancia con el principio de minimización del tratamiento. Por último, se añade un estándar de compatibilidad que debe ser tomado en cuenta al momento de dar una finalidad ulterior.

3.2. Estados Unidos: *California Consumer Privacy Act*

En este modelo se promueve, como pilar principal, el valor de la libertad personal frente a cualquier intervención Estatal.[82] Dado que la santidad de los hogares se ve amenazada por la administración, la autorregulación es una alternativa ágil y efectiva para la protección de derechos personales cuando la administración y la normativa resultan ineficientes en situaciones de complejidad técnica.[83]

Pese a este marcado modelo, se analizará la nueva ley de protección al consumidor de California, que presenta cambios disruptivos en este sistema. En el Estado de California se aprobó la CCPA en mayo de 2018, y entró en vigencia en enero de 2020. Respecto de esta, en primer lugar, se debe tomar en cuenta que es una ley con aplicación territorial restringida, únicamente para residentes del Estado de California. En segundo lugar, la aplicación material también es restringida, pues únicamente se protege a los residentes consumidores, no solo se limita personas físicas también incluye a personas jurídicas. En tercer lugar, aunque esta ley abarca a todo operador económico que trate datos personales de residentes en California, no todos pueden ser sancionados por la CCPA. Dependerá de ciertos criterios económicos establecidos en la ley, por lo que, por ejemplo, una compañía cuya utilidad no cumpla con el mínimo establecido, no está sujeta a esta regulación. Pese a estos obstáculos, esta ley es revolucionaria en este sistema al incorporar ciertos elementos del RGPD.[84]

El objetivo que persigue la CCPA es otorgar un control más efectivo al consumidor sobre sus datos personales que los operadores económicos recolectan. Nacen cuatro derechos que en el sistema estadounidense no se reconocían en materia de protección de datos personales.[85] Derecho del consumidor a conocer toda la información personal que se recopile sobre él. Derecho a conocer cómo es el tratamiento de sus datos personales. Derecho a suprimir información personal recolectada por las empresas. En caso de que un operador económico desee vender información del consumidor, nace el derecho a optar por no participar en esta transacción. El último derecho recogido es el derecho a la no discriminación por parte de empresas.

82 Piñar, "¿Existe privacidad?", 19.
83 Troncoso, "El desarrollo de la protección de datos", 36.
84 Laura Jehl y Alan Friel, "CCPA and GDPR Comparison Chart", s/f, 25 septiembre, 2020. https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf.
85 Xavier Becerra, "California Consumer Privacy Act", *Departamento de Justicia del Estado de California*, s/f, 25 septiembre, 2020. https://oag.ca.gov/privacy/ccpa.

3.2.1. Consentimiento

El RGPD opta por un sistema *opt in* donde debe mediar un consentimiento expreso, previo, informado, libre e inequívoco del titular. Por otro lado, en la CCPA la base del consentimiento gira en torno a un sistema *opt out*. Este es un sistema en el que se tratan datos personales del titular sin contar con su autorización, pero este puede optar por dar de baja sus datos personales a través de un sistema de exclusión de tratamiento.

Respecto del consentimiento, todos los negocios están obligados a informar a los consumidores sobre sus políticas de manejo de datos personales. Según la subsección 999.305 (a)(3), el aviso debe ser de fácil acceso y en un lenguaje sencillo para el consumidor.[86] Cuando se han recabado datos personales sin haber publicitado este aviso de exclusión, obligatoriamente, se requiere el consentimiento del consumidor. En el supuesto de dar a los datos recolectados un nuevo uso, en ese caso también se deberá notificar al consumidor para obtener su consentimiento. Ahora, por regla general, todos los datos personales pueden ser sujetos de venta. Sin embargo, existe un aviso de exclusión voluntaria donde el consumidor puede optar por la no venta de sus datos personales. Los datos personales únicamente pueden ser utilizados durante doce meses, período en el que expira el sistema *opt out*.

3.2.2. Finalidad

La CCPA no maneja un principio de finalidad y estándar, únicamente establece ciertas condiciones. Según la subsección 999.308, todo operador económico deberá notificar al consumidor cuál es su finalidad del tratamiento de datos a través de una política de privacidad.[87] Es obligación de la empresa identificar una categoría para cada dato personal recopilado. Se debe mencionar cuáles fueron las fuentes utilizadas para recabar la información, las finalidades comerciales o empresariales para las que se recopilaron los datos y los terceros ajenos a la compañía a los que se comparten estos datos. La falta de un principio rector y un estándar que limite el tratamiento de datos a una finalidad específica podría dar paso a injerencias y vulneraciones a la privacidad de los consumidores.

86 Subsección 999.305 literal a numeral 3, California Consumer Privacy Act [CCPA], Assambley Bill 375, 1 de enero de 2020.

87 Subsección 999.308, CCPA.

4. Proyecto de Ley Orgánica de Protección de Datos Personales

4.1 Estándar de protección: consentimiento y finalidad

Se debe partir del hecho de que las normas jurídicas responden a realidades sociales. ¿Cuál ha sido el contexto en el Ecuador para que no haya sido una necesidad social crear una norma de protección de datos? Puede que la responsabilidad sea compartida: Estado, empresas y ciudadanos, al no exigir una ley que delimite el ejercicio y regulación de este derecho. Aparte de la falta del desarrollo normativo, la doctrina y jurisprudencia respecto de esta temática es escasa en el país.

A pesar de lo dicho anteriormente, en Ecuador han existido distintos intentos por regular el derecho a la protección de datos personales a través de una ley específica.[88] Parte de la acción estratégica del Eje 6 del Plan Nacional de la Sociedad de la Información y el Conocimiento 2018-2021, es promulgar una ley orgánica de protección de datos personales.[89] El 19 de septiembre de 2019, el presidente Lenín Moreno envió a la Asamblea Nacional el Proyecto de Ley Orgánica de Protección de Datos Personales. El objetivo principal del proyecto es regular y proteger el ejercicio del derecho a la protección de datos personales.[90]

Además de la intención del Plan Nacional, la necesidad de contar con un cuerpo normativo nace de varias situaciones alarmantes. En septiembre de 2019, ZDNet dio a conocer que existió una filtración de datos personales, entre los que se encontraba información sensible de la población ecuatoriana.[91] Este no es un caso aislado. Todos los días se vulnera el derecho a la protección de datos personales. Por ejemplo, en tiendas digitales como OLX, Mercado Libre o tiendas físicas, especialmente en la bahía de Guayaquil, se venden bases de datos actualizadas de entidades públicas como el Consejo Nacional Electoral y la Dirección General de Registro Civil, Identificación y Cedulación.[92] En la mayoría de los casos, la recopilación y venta de los mencionados datos no es autorizada. La necesidad de contar con un cuerpo legal que mantenga un estándar de protección de datos personales que regule debidamente

88 Ecuador, Proyecto de Ley Orgánica de Protección de los Derechos a la Intimidad, y Privacidad sobre los Datos Personales, 2016.

89 Ministerio de Telecomunicaciones y de la Sociedad de Información, *Plan de la Sociedad de Información y del Conocimiento* (Quito, 2018), 74.

90 Artículo 1, Proyecto de Ley Orgánica de Protección de Datos Personales, Comisión Soberanía, Integración, Relaciones Internacionales y Seguridad Integral, Calificado por el CAL, 2019.

91 Ver, "La 'grave filtración' informática que expuso los datos personales de casi toda la población de Ecuador", *BBC News Mundo*, 16 de septiembre de 2019. https://www.bbc.com/mundo/noticias-america-latina-49721456.

92 Xavier Ramos, "Datos a la venta dan cuenta de que filtraciones no son nuevas en Ecuador", *El Universo,* 22 de septiembre de 2019. https://www.eluniverso.com/noticias/2019/09/21/nota/7527550/datos-venta-dan-cuenta-que-filtraciones-no-son-nuevas.

el consentimiento del titular y la finalidad del tratamiento de datos es urgente. A continuación, se analizará el estándar de protección de datos respecto del principio de consentimiento y finalidad que se propone en el Proyecto de Ley.

4.2. Consentimiento

El consentimiento es uno de los principios generales del derecho de protección de datos recogidos en el artículo 8 del Proyecto de Ley.[93] Su buen entendimiento es vital para garantizar este derecho fundamental.[94] Según el artículo 10, se puede legitimar el manejo de datos de distintas formas. Para efectos del presente trabajo, únicamente se analizará lo prescrito en el artículo 10 numeral 1, el "tratamiento solo será legítimo y lícito si cumple con [...] [el] consentimiento del titular para el tratamiento de sus datos personales".[95]

El legislador define al consentimiento como aquella "manifestación de voluntad libre, previa, específica, expresa, informada e inequívoca", [96] mediante la cual el titular autoriza al responsable el tratamiento de sus datos personales. Desde este punto, se introduce un estándar de protección que debe contar con seis características para que el consentimiento sea considerado válido.

La primera es la voluntad libre, sin vicios del consentimiento.[97] La pregunta a realizarse es, ¿cuáles son estos vicios del consentimiento? No se plasma una referencia específica en el Proyecto de Ley por lo que podría presumirse la existencia de un posible vacío legal. El Manual de legislación europea en materia de protección de datos menciona que se debe recurrir al Derecho Civil para hablar de consentimiento válido,[98] por lo que, en ese caso, la solución sería remitirse al Código Civil como norma supletoria. Entonces, si se toma como punto de partida la normativa civil en Ecuador, los vicios del consentimiento son los contemplados en el artículo 1467 del Código Civil: error, fuerza y dolo.[99] Esta característica se cumple cuando el consentimiento es libre de vicios del consentimiento en materia civil. Sería interesante si los legisladores, al debatir sobre el Proyecto de Ley, desarrollan un concepto específico desde una perspectiva autónoma de esta área del Derecho.

La segunda es la manifestación de voluntad previa.[100] Esta se verifica cuando el titular ha consentido antes del tratamiento. Caso contrario, si el consenti-

---

93 Artículo 8, Proyecto de Ley Orgánica de Protección de Datos Personales.
94 Susan Chen Mok, "Privacidad y protección de datos: un análisis de legislación comparada". *Diálogos Revista Electrónica de Historia* 11 (febrero 2010): 116, https://revistas.ucr.ac.cr/index.php/dialogos/article/view/6111/13852.
95 Artículo 8, Proyecto de Ley Orgánica de Protección de Datos Personales.
96 Id., Artículo 5.
97 Id., Artículo 14.
98 Agencia de los Derechos Fundamentales, *Manual de legislación europea,* 130.
99 Artículo 1467, Código Civil, R.O. Suplemento 104, de 20 de noviembre de 1970, reformado por última vez R.O. 526 de 19 de junio de 2015.
100 Id., Artículo 14.

miento es ulterior al tratamiento, se estaría frente a un tratamiento ilícito y no autorizado. Aunque el Proyecto de Ley se torna más flexible al establecer que existirán ciertas excepciones "cuando los datos personales no se obtuvieren de forma directa",[101] pueden ser consentidos por el titular con posterioridad.

La tercera es la especificidad del consentimiento. Esta se cumple si el titular tiene una referencia concreta de los medios y fines del tratamiento.[102] No se deduce de la simple lectura del Proyecto, si la voluntad del legislador es establecer el mismo requisito que establece en el RGPD o si se refiere al deber de información del responsable del tratamiento. De igual manera, es uno de los deberes más importantes del responsable del tratamiento, determinar cuáles son los mecanismos de tratamiento y la finalidad de este. Así se asegurará que el titular tenga conocimiento y control de sus datos personales. El consentimiento no puede ser específico si la información no conduce al titular a consentir una sola finalidad.

La especificidad se encuentra directamente relacionada con la cuarta característica: consentimiento informado. Esta se cumple cuando la información proporcionada va de conformidad con el principio de transparencia.[103] Es deber del responsable del tratamiento informar al titular de forma leal y transparente los fines del tratamiento, base legal, tipos de tratamiento, tiempo de conservación de los datos personales, entre otros.[104] Esta información debe ser proporcionada por cualquier medio, redactada en lenguaje claro, sencillo y de fácil comprensión. En caso de que la información no se brinde conforme lo prescribe la norma, se entenderá que el consentimiento no es informado, no cumpliéndose con la cuarta característica.

Las dos últimas características del consentimiento son: una manifestación expresa e inequívoca. A comparación de las dos características presentadas anteriormente, su validez depende totalmente de la manera en cómo el titular da a conocer su aceptación para el tratamiento de sus datos personales. Esto se puede dar a través de una declaración clara y afirmativa o se puede deducir de una acción. Por un lado, al hacer alusión a la manifestación de la voluntad expresa, significa que el responsable del tratamiento de datos personales de manera indubitable podría demostrar la voluntad del titular de consentir el tratamiento.[105] Por otro lado, es inequívoca cuando no queda duda alguna sobre el alcance del consentimiento del titular para que el responsable pueda tratar sus datos. En caso de que exista alguna duda sobre la intención del titular en consentir al tratamiento de sus datos personales, no se podrán cumplir con estas dos características.

101 Id.
102 Id.
103 Id., Artículo 14.
104 Id., Artículo 23.
105 Id., Artículo 14.

El Proyecto de Ley establece seis características, de inexorable cumplimiento, para que se pueda considerar válida la manifestación de la voluntad del titular para que alguien pueda tratar o comunicar sus datos personales. Si no se cumple una de estas características, se estaría hablando de un tratamiento ilegítimo. En caso de que se apruebe el Proyecto de Ley, será interesante analizar cómo las empresas y responsables del tratamiento manejarán e implementarán este estándar, que contiene dos elementos adicionales al RGPD.

4.3. Finalidad

A diferencia del principio del consentimiento del titular, el cumplimiento de este principio recae en su totalidad sobre el responsable del tratamiento de datos. Según lo prescrito en el artículo 11 del Proyecto de Ley, la finalidad del tratamiento de datos personales deberá ser: determinada, explícita y legítima. Además, el responsable del tratamiento no podrá dar un fin distinto al manifestado inicialmente. Aunque se prevé que, en ciertas ocasiones, se pueda dar una finalidad distinta a la inicial, siempre y cuando este nuevo tratamiento sea conforme con el principio de legitimidad.[106]

Para que una finalidad sea válida se deben cumplir estas tres características. Por un lado, se entiende por determinado que el responsable del tratamiento de datos especifique en el fichero de datos la finalidad y los mecanismos de tratamiento. En caso de que la información contenida en el fichero no esté encaminada a una única finalidad, no sería válida. Por otro lado, es explícita cuando se ha informado al titular sobre toda la información concerniente al tratamiento de sus datos. Sin embargo, en caso de que no se ponga a su disposición toda la información, su consentimiento podría carecer de información y especificidad, viciando el consentimiento y dando como resultado un tratamiento ilegítimo. Por último, se entiende por legítima cuando la finalidad del tratamiento de datos se adecúa a lo prescrito en el ordenamiento jurídico. Si no se cumplen las condiciones requeridas en la normativa, se hablaría de una finalidad ilegítima.

Al principio de finalidad se lo debe analizar junto con los principios de juridicidad, lealtad y transparencia, pertinencia y minimización de datos. De conformidad con lo que manifiesta el principio de juridicidad, lealtad y transparencia recogidos en el artículo 9 del Proyecto de Ley, los datos personales no pueden ser tratados, bajo ninguna circunstancia, para fines y con medios ilícitos o desleales. Del mismo modo, el artículo 12 prescribe que los datos personales deben ser pertinentes y limitados a lo mínimo necesario para la finalidad de obtención.[107] La aplicación concordante y sincronizada de estos

106 Id., Artículo 11.
107 Id., Artículo 12.

principios se presenta como una preocupación fundamental. El responsable no podrá procesar los datos para una finalidad diferente o que sea incompatible con el estándar. Además, es su deber controlar que los datos personales sean adecuados, pertinentes, actualizados y no excesivos con relación a la intención de obtención y tratamiento de datos.

El proyecto de ley reconoce a la finalidad del tratamiento de datos personales como un principio rector. En primer lugar, en el artículo 8, se establecen los principios que regirán la normativa.[108] En segundo lugar, en el artículo 11, se define el principio, sus características y condiciones para que este sea válido.[109] El objetivo principal de este principio y el estándar que se busca mantener tienen una función informadora e integradora.[110] Respecto de la función informadora, es obligación del responsable especificar en el fichero de datos toda la información pertinente y adecuada para el tratamiento de datos. A su vez, la función integradora busca que este derecho se convierta en un sistema hermético en su aplicación armónica con los principios mencionados anteriormente.

4.4. Críticas y propuestas al Proyecto de Ley Orgánica de Protección de Datos Personales

Previamente, se analizó cómo se tratan los datos personales en dos sistemas normativos y cómo lo pretende abordar el Proyecto de Ley. En esta sección se hará una comparación de los estándares que proponen los tres cuerpos normativos para determinar cuál es el que se pretende incorporar en nuestro ordenamiento jurídico y qué tan eficiente podría llegar a ser. Por último, se hará un breve análisis con críticas y propuestas al cuerpo normativo en estudio.

Sobre el primer punto, el RGPD ha desarrollado un estándar de protección alto. El consentimiento del titular es la piedra fundamental para legitimar el tratamiento de datos, pese a existir otros mecanismos de legitimación. El cumplimiento de la finalidad del tratamiento de datos personales debe cumplirse estrictamente, caso contrario se hablaría de un tratamiento ilegítimo o no autorizado. Existe una autoridad de protección de datos que se encarga de velar por el cumplimiento de la normativa de cada país con la finalidad de que no se vulnere este derecho fundamental.

En segundo plano, se analizó el sistema de protección de datos en Estados Unidos. No existe una ley federal que regule y proteja el ejercicio de este derecho fundamental. Es más, es el propio titular quien debe autorregular este derecho y, en caso de vulneración, deberá acudir al sistema judicial para soli-

108 Id., Artículo 8.
109 Id., Artículo 11.
110 Adrián Palma Ortigosa, "Principios relativos al tratamiento de datos personales", en: *Protección de datos, responsabilidad activa y técnicas de garantía*, ed. Juan Pablo Murga Fernández (Madrid: Editorial Reus, 2018), 40.

citar la reparación de daños y perjuicios. Sin embargo, ha nacido una nueva iniciativa en California. La promulgación de la CCPA toma en cuenta ciertos elementos del RGPD, dando vida a cuatro nuevos derechos que no se habían contemplado previamente en este sistema. Sin embargo, sigue siendo un estándar pobre de protección de datos.

En cambio, en Ecuador, se puede ver que el Proyecto de Ley delimita ciertos conceptos base, establece principios de aplicación directa, que establecen derechos de los titulares y obligaciones de los responsables del tratamiento de datos. Entre estos principios se observa que el consentimiento es una de las maneras de legitimar el tratamiento de datos, mismo que contiene un estándar de protección detallado y específico. Por otro lado, la finalidad del tratamiento es otro principio indispensable al momento de procesar o manejar datos personales. Se establece una Autoridad Reguladora que será analizada posteriormente.

A continuación, una comparación de los estándares que establece cada cuerpo normativo:

5. Cuadro 1: Comparación de estándares en legislación comparada

	RGPD	CCPA	Proyecto de Ley
Formas de legitimar el tratamiento	Seis:[111] el consentimiento es la regla general.	No hay requisitos legales.	Siete:[112] el consentimiento es parte de ellos.
Características del consentimiento	Cuatro:[113] libre, específico, inequívoco e informado.	Sistema *opt out*,[114] sistema de exclusión en la venta de datos personales.	Seis:[115] libre, previo, específico, expreso, informado e inequívoco
Características de la finalidad	Tres:[116] determinada, explícita y legítima.	No hay un estándar.	Tres:[117] determinada, explícita y legítima.

A lo largo de este artículo se ha podido observar que, dentro de esta revolución normativa que se está dando a nivel mundial, el ordenamiento jurídico

111 Artículo 6, RGPD.
112 Artículo 10, Proyecto de Ley Orgánica de Protección de Datos Personales.
113 Artículo 4 numeral 11, RGPD.
114 Subsección 1798.120 literal a, CCPA.
115 Artículo 5, Proyecto de Ley Orgánica de Protección de Datos Personales.
116 Artículo 5 numeral 1 literal b, RGPD.
117 Artículo 11, Proyecto de Ley Orgánica de Protección de Datos Personales.

ecuatoriano busca alinearse e inclusive superar al estándar europeo. Aunque se debe tomar en consideración que el Proyecto de Ley presenta distintas variantes. Esto genera una serie de preguntas que buscan dar respuesta a qué tan bueno podría resultar alinearse a este estándar de protección de datos.

La primera pregunta por plantearse, ¿se puede considerar que el Ecuador tendrá un nivel adecuado de protección de datos? Según Serrano, para que un país tenga un nivel adecuado de protección se necesitan tres elementos:[118] 1) normativa que garantice el ejercicio de este derecho fundamental; 2) una autoridad estatal independiente; y 3) normativa especializada en protección de datos.

En este momento, es pertinente enfocarse en el primer y tercer requisito, el segundo será analizado posteriormente. El Proyecto de Ley que actualmente se está discutiendo en la Asamblea Nacional, será el cuerpo especializado en regular esta materia. Su objetivo principal es "regular el ejercicio del derecho a la protección de datos personales, la autodeterminación informativa, […] a través del desarrollo de principios, derechos, obligaciones y mecanismos de tutela".[119] De esta manera, se garantizará un ejercicio efectivo de este derecho fundamental a través de una norma especializada.

Esto conduce a una segunda pregunta, ¿qué tan eficiente puede resultar un estándar de protección tan elevado en el Ecuador? La eficiencia recae en cómo se traslada el estándar de protección establecido en el RGPD al Proyecto de Ley. Se puede ver que el legislador contempla todos los mecanismos de legitimación del tratamiento establecidos en el RGPD e incorpora dos elementos adicionales. Respecto del consentimiento se han establecido las cuatro características del estándar del RGPD, pero se añaden dos características adicionales. Por último, las características del estándar de finalidad siguen siendo las mismas en ambos cuerpos normativos.

A primera vista se podría asegurar que será un estándar sólido. De hecho, en ciertos aspectos es más exigente que el RGPD. Sin embargo, hay una diferencia entre el ser y el deber ser, cuando se trata de la vigencia, validez y eficiencia de una ley. Para poder determinar qué tan acatado será este estándar y en qué medida, es necesario que se apruebe el Proyecto de Ley y se observe el período de transición para evaluar realmente los resultados.

Sobre el segundo punto de debate, para poder realizar críticas y propuestas al Proyecto de Ley, se debe responder, ¿más allá del Proyecto, está lista la sociedad ecuatoriana para este cambio tan drástico? Para responder esta interrogante, se debe observar la evolución de este derecho en el ordenamiento

118 Rafael Serrano Barona, "*Datos Personales en Ecuador: Análisis del Proyecto de Ley de Protección de Datos Personales*" (Conferencia, AMCHAM Guayaquil, 6 de agosto de 2020).

119 Artículo 1, Proyecto de Ley Orgánica de Protección de Datos Personales.

jurídico. Recién en el año 2008 la Constitución lo reconoció como un derecho constitucional, es decir que se trata de un derecho relativamente nuevo en este sistema. Puede resultar bastante prometedor que el Proyecto de Ley se desarrolle de conformidad con el estándar establecido en el RGPD. No obstante, se debe tomar en consideración que la Unión Europea ha desarrollado el régimen de protección de este derecho durante alrededor de 40 años.[120] En Ecuador esto es algo incipiente. Muy poco se conoce y ha sido estudiada esta área del Derecho, por lo que implementarlo será una tarea y un reto bastante complejo.

Dependerá de muchos factores el conseguir alinearse al estándar europeo. Uno de los principales, será la educación. Será esencial que la autoridad competente eduque tanto a los titulares como a los responsables y encargados. Al no existir consciencia y cultura sobre esto, el esfuerzo por educar a cada individuo ayudará a impregnar el derecho de protección de datos como parte de la idiosincrasia ecuatoriana. Difundir a través de campañas y capacitaciones conceptos básicos e importantes en esta materia, derechos de los titulares, obligaciones de encargados y responsables, y mecanismos adecuados.

En definitiva, ¿existen mecanismos adecuados y pertinentes para esta transición? En líneas precedentes, se mencionó que Serrano establece tres elementos para que un que un país tenga un nivel óptimo de protección de datos.[121] Es aquí donde se analizará el segundo elemento: una autoridad estatal independiente. La autoridad de protección de datos personales debe ser una entidad de derecho público, con autonomía administrativa y financiera, además de contar con personería jurídica. No debería tener relación de subordinación o jerarquía con la administración central. En contraposición con lo dicho, el artículo 88 del Proyecto prescribe que se creará una Autoridad de Protección de Datos Personales dependiente de la Función Ejecutiva.[122] La tendencia actual es reducir las autoridades o dependencias del Estado. Además, dada la situación económica y el contexto social del país, no será fácil crear una autoridad independiente. Probablemente por este factor se podría presumir que la solución sería crear un órgano adjunto a la DINARDAP.

Esta dependencia podría afectar la seguridad jurídica y el pleno ejercicio de este derecho fundamental. El artículo 89 del Proyecto de Ley establece una serie de funciones, atribuciones y deberes que se resumen en supervisión, control, evaluación, autorización y normativa. Considerando estas características sería más plausible que la entidad, en todo caso, forme parte de la Función de Transparencia y Control Social. De esta manera el cuerpo colegiado podría

120 Luis Enríquez Álvarez, "La visión de América Latina sobre el Reglamento General de Protección de Datos", *Comentario Internacional. Revista Del Centro Andino De Estudios Internacionales* 19 (Julio 2020): 100, https://doi.org/10.32719/26312549.2019.19.4.

121 Serrano, "*Datos Personales en Ecuador*".

122 Artículo 88, Proyecto de Ley Orgánica de Protección de Datos Personales.

conformarse por representantes del sector público, privado y académicos. La elección de estos sería mediante un proceso de méritos y oposición en el que se evalúe tanto la formación profesional como la experiencia en esta materia.

Por último, se aseguró que, al contar con un estándar adecuado de protección de datos, se busca atraer a la inversión extranjera. ¿Será posible llevar a cabo esta aspiración? La respuesta es, no necesariamente. A diferencia de lo establecido en el RGPD, en el capítulo XI del Proyecto de Ley se establece un régimen de sanciones con una base mínima y un valor máximo, los cuales resultan bastante elevados para el sector privado. Estas multas pueden ascender hasta el 17% del volumen del negocio. El artículo 86 prescribe que el volumen de negocio son los ingresos de la compañía antes de la conciliación tributaria,[123] por lo que prácticamente se estaría hablando de ingresos brutos. Tener multas y sanciones excesivas y no proporcionales desincentivan al inversor a constituir empresas en el Ecuador.

Es cierto que debe realizarse una ponderación entre contar con un estándar adecuado que garantice y proteja efectivamente al derecho a la protección de datos, frente a un estándar que llame la atención del inversor extranjero. No se debería sacrificar este derecho fundamental por intereses meramente económicos, dejando de lado los fines del Estado de proteger a la sociedad. La norma no es clara con los términos de las sanciones y se deja un espacio de discrecionalidad amplio a la autoridad, que deberá ser limitado por los principios propios del Derecho Administrativo.

6. Conclusiones

Se mencionó que los datos personales son el nuevo petróleo del internet y la nueva moneda de la economía digital. Este avance desenfrenado de la tecnología puede acarrear ciertas vulneraciones, lo que ha generado que la normativa de protección de datos se adapte a este fenómeno. Ha nacido la necesidad de contar con un estándar adecuado de protección que genere equilibrio entre protección de este derecho fundamental, desarrollo económico e innovación. Esto se lo puede conseguir a través de dos modelos regulatorios: europeo y estadounidense.

El estándar europeo de protección de datos, evidentemente, es más estricto que el implementado en Estados Unidos. Su objetivo es generar un espectro de seguridad robusto en la protección de la privacidad, tratamiento y circulación de datos, pues el modelo americano ha puesto en evidencia que un sistema de protección de datos que se basa únicamente en la autorregulación del titular podría presentar limitaciones. La CCPA y su intento de acercarse

123 Artículo 86, Proyecto de Ley Orgánica de Protección de Datos Personales.

al modelo de protección de datos de la Unión Europea, el cual se basa en la regulación por parte de una autoridad encargada, en el fondo representa el reconocimiento del fracaso del sistema de autorregulación. Esta diferencia es el principal motivo para que Ecuador, y otros países, busquen implementar lo estandarizado en el RGPD e inclusive superarlo.

Se analizó que el estándar que propone el Proyecto de Ley podría llegar a ser más riguroso que el establecido en Europa. Este establece ciertos elementos adicionales que en el RGPD no se han contemplado. Este es el marco referencial para esta iniciativa legal, aunque en ciertos puntos como en el principio de finalidad, se han tomado los mismos parámetros. La única manera de poder tener una respuesta certera de si esto se adaptará o no a la realidad, es que efectivamente se promulgue y se ejecute lo contemplado en esta futura Ley Orgánica de Protección de Datos Personales.

Con base en esta necesidad por regular adecuadamente el derecho a la protección de datos en la sección de críticas y propuestas, se demostró que para llegar a tener una ley eficiente son varios los aspectos a tomar en cuenta. Entre estos factores se mencionaron la educación y cultura legislativa, Autoridad de Protección de Datos y sanciones. Se recomienda al legislador realizar un análisis de impacto regulatorio. Esta es una herramienta que permite evaluar las propuestas normativas. Así se puede examinar cuáles serán los beneficios, costos y efectos potenciales que el Proyecto de Ley tendrá en el ordenamiento jurídico. De esta manera, estas deficiencias que el actual borrador de ley presenta podrán ser resueltas.

Existe bastante desarrollo sobre la teoría de protección de datos personales en la que se describe a los principios de manera abstracta. Un ejemplo claro es el presente trabajo, en el que hay un amplio análisis del estándar que manejan distintos modelos normativos. Sin embargo, es difícil encontrar publicaciones que hablen sobre los principios analizados y la conexión con la práctica y vida diaria. Incluso, se podría analizar y evaluar la efectividad de los principios estudiados en el tratamiento de datos personales.

Por último, el desarrollo tecnológico como el manejo de *big data*, lleva a cuestionarse y a evaluar estos esquemas, ¿estos principios realmente son los ejes centrales del derecho de protección de datos? ¿qué principios serán determinantes en el futuro? ¿estos esquemas dejarán de lado a la autodeterminación informativa y privacidad por consentimiento? ¿el énfasis actual del derecho de autodeterminación informativa ha generado una fatiga en el principio de consentimiento? Son temas que deben ser analizados en trabajos posteriores, ya que realmente aportarían a la discusión actual de esta materia. Pero por el momento es importante destacar que esta iniciativa legislativa busca tanto proteger este derecho fundamental como dar seguridad jurídica a compañías.